Homeland Security Airport Security Model

Norman F. Schneidewind
IEEE Congressional Fellow, IEEE Fellow
Professor of Information Sciences, Naval Postgraduate School
nschneid@nps.navy.mil

Abstract

This model provides a framework for helping to understand and analyze the airport security problem. By modeling the security process, and identifying the weak points, we were able to make recommendations for possible Federal initiatives through legislative or management action to close the identified security loopholes. Passenger flow through the ticket counter, security station, and gate, which potentially includes terrorists, is modeled and quantified. A probability model estimates the probability of a terrorist escaping detection at the various stations. This probability is a function of the reliability of a proposed security database and the reliability of security equipment. The influence of these reliabilities on the probability of *non detection* is studied. In addition, a commonly overlooked security problem -- overloading security personnel with passenger traffic to the extent that they are distracted from thoroughly checking passengers -- is modeled and analyzed. Model quantitative results are used to delineate the implications for changes in security policy at the nation's airports.

Introduction

A model of airport security is proposed and executed. The model involves the flow of a group of passengers, who wish to board a given aircraft, to ticket counters, security stations, airline gates, and aircraft. By confining the security problem in this way, the very difficult problem of airport security analysis is simplified. Why do we develop such a model? An important reason is: "Airports and ticket counters have been attacked, and even airline offices have not been spared in terrorist attempts to intimidate governments and prevent the western public from flying. Terrorists simply cannot leave airports alone, nor does it make sense to do so, since they are the weak point in Western defenses" [JOH91]. And this was written before 9/11! By way of historical perspective, in 1973 the Federal Aviation Administration (FAA) specified that the three critical security areas in airports are the ticket counter, boarding gate, and the aircraft [JOH91]. Curiously, the security station (i.e., luggage x-ray station) is omitted.

According to [JOH91], technology has not kept pace with the threat: terrorists exploit existing technology, airports upgrade their technology, but terrorists outwit that technology, in a never-ending cycle. "we will always be in a position where deterrence presupposes a rational adversary" [JOH91].

This model contains new concepts as follows: improve the reliability of airport security equipment; implement a security database in airports that do not have this capability; improve the reliability of security databases in airports where they exist; and alleviate queuing problems at airline passenger stations and airport security facilities. If these measures are implemented by Congressional funding and enabling legislation, the threat of terrorist attacks should be reduced at the nation's airports.

The severity of the problem is dramatized by the following findings:

Pre 9/11 Aviation Unpreparedness

WASHINGTON - The Federal Aviation Administration received repeated warnings in the months prior to Sept. 11, 2001, about al-Qaeda and its desire to attack airlines, according to a previously undisclosed report by the commission that investigated the terror attacks [MSN05].

The report by the 9/11 commission that investigated the suicide airliner attacks on the World Trade Center and the Pentagon detailed 52 such warnings given to FAA leaders from April to Sept. 10, 2001, about the radical Islamic terrorist group and its leader, Osama bin Laden. The commission report, written last August, said five security warnings mentioned al-Qaeda's training for hijackings and two reports concerned suicide operations not connected to aviation. However, none of the warnings pinpointed what would happen on Sept. 11. FAA spokeswoman Laura Brown said the agency received intelligence from other agencies, which it passed on to airlines and airports. But, she said, "We had no specific information about means or methods that would have enabled us to tailor any countermeasures." Brown also said the FAA was in the process of tightening security at the time of the attacks. "We were spending $100 million a year to deploy explosive detection equipment at the airports," she said. The agency was also close to issuing a regulation that would have set higher standards for screeners and, for the first time, give it direct control over the screening work force. [911] However, there are few airports, today, that have explosive detection equipment installed. In addition, simulated tests have shown that it is possible to pass screener detection in major U.S. airports, while carrying concealed weapons. Thus, the need for a model that can pinpoint vulnerabilities in airport security.

Findings from the 9/11 Commission: [911]

- Aviation officials were "lulled into a false sense of security" and "intelligence that indicated a real and growing threat leading up to 9/11 did not stimulate significant increases in security procedures."
- Of the FAA's 105 daily intelligence summaries between April 1, 2001, and Sept.10, 2001, 52 mentioned Osama bin Laden, al Qaeda, or both, "mostly in regard to overseas threats."
- The FAA did not expand the use of in-flight air marshals or tighten airport screening for weapons. It said FAA officials were more concerned with reducing airline congestion, lessening delays and easing air carriers' financial problems than thwarting a terrorist attack.
- A proposed rule to improve passenger screening and other security measures ordered by Congress in 1996 had been held up by the Office of Management and Budget and was still not in effect when the attacks occurred, according to the FAA.

Passenger and Baggage Screening

The Aviation and Transportation Security Act (ATSA) made overall aviation transportation security a direct federal responsibility for the first time [DHS05]. The Transportation Security Administration's (TSA) responsibilities include ensuring screening of passengers through a mix of federal and private screeners and technology. The screener workforce consists of 45,000 screeners located at 448 airports. The screeners are supported by

technology, including x-ray machines, explosive trace detection machines, and explosive detection systems. U.S. air carriers transport 12.5 tons of cargo, 2.8 tons of which is secured on passenger planes. The remaining 9.7 million tons is shipped in cargo planes; air freight remains a serious threat to the nation. TSA is charged with closing this security vulnerability. While obviously important, air freight security is beyond the scope of this research.

Despite all of the above, according to [BEN05], "We are spending nearly $5 billion each year on passenger and baggage screening systems, yet lethal weapons still are getting past security and onto planes. While we have devoted enormous attention and resources to improving aviation security, it is still far too easy for a terrorist to get a weapon on a passenger plane. The Department of Homeland Security (DHS) Inspector General, the Government Accountability Office (GAO), and the TSA have conducted tests on TSA screeners at the nation's airports and found surprisingly high failure rates. An alarming number of prohibited items are still not being detected during checks of passengers, carry-on items, and checked baggage". In addition, according to [CKE05], DHS has been slow to deploy equipment and technology that could aid airport screeners in detecting concealed weapons and explosives.

Air Cargo

"While airline passengers may be screened, cargo beneath their feet is not. The TSA has identified two critical risks to air cargo "(1) The hostile takeover of an all-cargo aircraft leading to its use as a weapon; and (2) the use of cargo to introduce an explosive device onboard a passenger aircraft in order to cause catastrophic damage. Terrorists have exploited the lack of cargo security on several occasions. For example, a device in a baggage container of Pan Am Flight 103 caused the flight to explode in 1988 over Lockerbie, Scotland.4. An explosion aboard a U.S. airliner in 1979 was caused by a parcel linked to the "Unabomber" Theodore Kaczynski and shipped as air cargo. While Congress has mandated tripling air cargo screening, a large portion of commercial air cargo remain unscreened. TSA relies heavily on the "Known Shipper" program, under which only approved companies may ship cargo on passenger aircraft. A company can become a "Known Shipper" with practically no security checks" [BEN05].

PRINCIPLES OF MODELING AND SYSTEMS ENGINEERING

Since modeling is the central tool used in this research, it is appropriate to outline the methodology and spirit of this quantitative approach to problem solving. In particular, we describe the operations research (OR) approach to model development [HIL01] and systems thinking as exemplified in the field of systems engineering [TUR93]. First, we outline the steps in an OR study, annotated with the relevance to the airport security model.

1. Define the problem of interest and gather relevant data.

   The problem of interest is to improve the security of the nation's airports. An important facet of problem definition is to identify the decision makers. For airport security, these are the managers in the FAA, TSA, and airport and airline executives.

   Unfortunately, with few exceptions, there is not much published data on airport security available. Our search of the Transportation Research Information Services and the Transportation Research Board. databases did not yield relevant data, such as airline terrorist threat incidents. Thus, we resort to the use of randomized

hypothetical, but realistic data, and sensitivity analysis to compensate for the data void. We also subject the model to extreme value testing (e.g., using values of probability of terrorist *non detection* that seem unlikely, but, nevertheless, might occur in an airport security system), as a form of sensitivity analysis, to note the effect on the solution [HIL01].

2. Formulate a mathematical model to represent the problem.

   Since little is known with certainty about the details of the airport security problem, we use a probabilistic approach to estimating the quantities of interest, such as the probability of *not* detecting a terrorist by the time he reaches the gate, if he has not been detected prior to this point. No model can be a complete representation of the real system. If it were, it would be incomprehensible and mathematically intractable. Thus, we extract from the real world of airport security the key factors, such as the probability of *non detection*, as opposed to attempting to model every movement of a terrorist in an airport. Note that our focus is on *non detection* because we wish to emphasize the probability of a terrorist escaping apprehension.

3. Develop a computer-based procedure for deriving solutions to the problem from the model.

   A spreadsheet approach is used because sensitivity analysis of the solutions can be performed conveniently and plots of the solutions can be obtained easily.

4. Test the model and refine it as needed.

   Although we are unable to test the model in an airport at this time, we perform reality checks on the solutions. That is, we check the model assumptions, solutions, and sensitivity analyses to see whether they comport with reality (e.g., a solution of 99.9% probability of terrorist detection would be considered unrealistically optimistic). If such a solution emerged, we would modify the model to produce a more realistic result.

5. Prepare for the ongoing application of the model as prescribed by management.

   This step is beyond the scope of this research because, at this stage, the model is a proposal that may be considered for implementation by FAA, TSA, and airport, and airline managers. The details of implementation would be a decision taken by theses managers.

6. Implement the model.

   Examples of implementation details are the following: training of airport personnel in the revised passenger security process, implementing the security database and terrorist detection procedures, and installing equipment to detect biological, chemical, and nuclear weapons. Biological agents and toxins are of particular concern [CSI04].
   A key piece of legislation pertaining to biological terror is the Intelligence Reform and Terrorism Prevention Act of 2004 that contains various provisions to promote and accelerate the use of biometric technology for secure identification. The law provides for the use of biometric technology in airport access control and law enforcement travel [USS05].

Systems Engineering Concepts

Now, we explore how systems engineering concepts can be applied to airport security. In this vein, an aspect of the origin of systems thinking was the realization that that particular objects are comprised of components and these components are interrelated and independent [TUR93]. The following Table 0 portrays the airport security example, showing current security holes that could be rectified by using a database ID check at the Security Station and Gate:

Table 0. Airport Security Object				
Components		Related By	Security Control	
		Boarding Pass and ID	Database	Security Equipment
Ticket Counter		x	x	Does not apply
Security Station		x	**Security Hole**	x
Gate		x	**Security Hole**	Does not apply
Passengers		x		
Non Terrorists	Terrorists	x		

One of the critical developments relative to the origins of systems thinking is that of *cause* and *effect*. When a particular component behaves in a certain way, a different component in the related object reacts in a predictable way. [TUR93] For example:

If a passenger (component P) fails a database ID check, then an agent (component A) reacts to detain component P.

Furthermore, the behavior of component P can only be understood by identifying and characterizing the impact of components on each other (e.g., component A checks the database) and the influence of the components on the object (i.e., airport security system) [TUR93].

OBJECTIVE

According to [HIL01], the first order of business in an OR study is to define the objective. Accordingly, we state that our objective is to identify weak points (e.g., security station check) and links (e.g., passenger flow between security check station and gate) in the security process for the purpose of influencing government legislation and regulations to strengthen the process. We feel the subject of this research is extremely important because "America is not sufficiently prepared to fully respond to a catastrophic terrorist attack on U.S. soil that involves chemical, radiological, or nuclear weapons" [CSI04].

MOTIVATION

Consistent with the objective, we relate our experience at an airport that indicates the need for improvement in airport security. Instead of focusing on security measures, like a high reliability and comprehensive security database, which would significantly enhance security, the TSA, in some instances, spends considerable time on trivial matters. For example, we were recently passengers at the one of the nation's airports. We were carrying a stapler in our briefcase. After the case went through the x-ray machine, and signaled an alert, the TSA agent asked to

open the case. She saw that the "offending object" was the stapler. She then removed the stapler from the case, put it in a basket, and sent the case and basket through the x-ray machine *again*. It seemed obvious that the only object in the case -- the only metal object -- that could have signaled an alert was the stapler. Thus, the process should have stopped after the case was opened. Instead of paying TSA personnel to spend time on trivial searches, the TSA should invest in a security database and in improving the reliability of security station equipment.

In addition to seemly non productive security processes, as described above, certain proposed legislation, does not appear to be helpful. For example, a provision of immigration bill HR418, which passed the House of Representatives, would require: "that information on anyone convicted of using a false driver's license to board an airplane be added to aviation security screening databases" [HOU05]. The trouble with this provision is that it "closes the barn door after the horse is out of the barn". No terrorist is going to try to use the same identification again, if his identification had been discovered as false! It is important to note that there have been proposals for standardizing the driver's license [WAR05], which could become, in effect, a national identification card. With such a card, it would be difficult to fake identification; thus, the probability of *non detection* would be decreased. This is an issue currently being debated by Congress. It is not clear that such legislation will be passed because of the opposition of privacy advocates.

Other examples of airport security problems that motivate our research are the following:

Background on Airport Security Issues

Selected Items from Terrorist Detection History

This section illustrates why airport security is a problem and why we are motivated to study the problem. A critical aspect of successful terrorist and weapons detection is the quality and appropriateness of the detection tests. The following reports from the media illustrate some of the problems in conducting successful tests:

HOW NOT TO TEST AIRPORT SECURITY, SCHNEIER ON SECURITY, DECEMBER 20, 2004[BBC05]

If this were fiction, no one would believe it. Four days after police at Charles de Gaulle Airport slipped some plastic explosives into a random passenger's bag as part of an exercise for sniffer dogs, it is still missing -- and authorities are stumped and embarrassed. It is perfectly reasonable to plant an explosive-filled suitcase in an airport in order to test security. It is not okay to plant it in someone's bag without his knowledge and permission. (The explosive residue could remain on the suitcase long after the test, and might be picked up by one of those trace mass spectrometers that detects the chemical residue associated with bombs.) But if you are going to plant plastic explosives in the suitcase of some innocent passenger, shouldn't you at least write down which suitcase it was?

US airport security loses 'bomb' [BBC05]

Security screeners at a US airport lost track of a bag containing fake explosives and allowed to be loaded on a flight to Amsterdam. The "bomb" was planted in luggage for training exercise at Newark Liberty International Airport. A scanning machine raised the alarm, but the bag was not searched and airport staff lost track of it. "At no time did the bag pose a threat and at no time was anyone in danger," said a transport security spokeswoman.

Airport Security Data

Since, with certain exceptions, airport security data is either classified or unavailable, we have had to resort, in this model, to use hypothetical but realistic data to illustrate the principles of the model. See the Appendix for the spreadsheet data and the results of *example* computations. In future research, we will attempt to collect data about security attacks from reports, web sites, and the Department of Homeland Security DHS).

Information flow rates, queue characteristics, etc., which are used in the analytic model, are expected or mean values. If instantaneous values of these variables are desired, simulation must be used. The values of quantities used in the examples are for illustrative purposes. Sensitivity analysis is performed to protect against choosing certain values in the examples. As Cordesman points out, probabilities based on history may be worthless (e.g., pattern of past no indicator of 9/11 attack). It is better to use "what if" analysis [COR, p. 25]. It is important to consider worst case scenarios [COR, p. 33]. Many of the model variables are randomized to provide further protection again bias. An example of "what if "analysis is covered in the What If section.

Threats

Now, we consider the flow of passengers, wherein one or more could be terrorists, and a threat to innocent passengers, through the ticketing, security checking, and boarding process, as depicted in Figure 0.

Definitions

Refer to Figure 0 when reading the definitions:

Facilities: ticket counter (A), security station (S), and gate (G).

P_t is the probability that a passenger (on the aircraft) is a terrorist, mean ≈ .05 [CRS04], N is the estimated number of possible terrorists who are ticketed on Plane P (N is assumed to be in the range 1,,,10), and C is the capacity of P. A mean value for P would be appropriate to use, if C were a constant. However, just considering the Boeing Company alone, there are ten commercial models, with the capacity in number of passengers, shown in Table 1 [BOE05]. Therefore, it is appropriate to consider P_t as a variable, and to calculate it as $P_t = N / C$.

Table 1. Boeing Company Commercial Aircraft Models

Model	Capacity (C = number of passengers)
717	106
737	189
747	524
757-300	280
757-200	228
767	375
777	550
787-3	296
787-8	223
787-9	259

P_A is the probability that the terrorist will be detected at the ticket counter by querying the security database. Specifically, this probability is a function of the accuracy and completeness of the security database and of the type of identification I_A presented by the passenger at the ticket counter. Although the probabilities of detection at the ticket counter, security station, and gate differ in the real world, they are treated as equal in this model because 1) we have no evidence to the contrary and 2) the assumption of equality is mitigated by randomizing these quantities in the model.

The probability that the terrorist will be detected at the ticket counter is of particular relevance in light of the El Al airlines practice of requiring complete identification of the passenger when purchasing a ticket to allow security officials to compile a reference file on the passenger [JOH91]. Although this is an excellent practice, it is not clear that it would be acceptable to American airline passengers.

R_d is the reliability of the security database. Specifically, this is the probability of the database operating without failure during the security checks at the three stations. It is assumed that the reliabilities at the three facilities are equal, since this feature is new in airports, with little information available about operating characteristics.

P_S is the probability that the terrorist will be detected at the security station by querying the security database or by performing the luggage check. Specifically, this probability is a function of the accuracy and completeness of the security database and of the type of identification I_S presented by the passenger at the security station *and* the accuracy of the luggage checking equipment.

Rs is the reliability of the security checking equipment. Specifically, this is the probability of the security checking equipment at the three facilities operating without failure during the security checks. As in the case of R_d, it is assumed that the reliabilities at the three facilities are equal, because we have no information to the contrary.

P_G is the probability that the terrorist will be detected at the gate by querying the security database. Specifically, this probability is a function of the accuracy and completeness of the security database and of the type of identification I_G presented by the passenger at the gate.

In later sections, we use the following additional definitions:

P_{Af}, probability of *non detection* at the ticket counter.

P_{Sf}, probability of *non detection* at the security station.

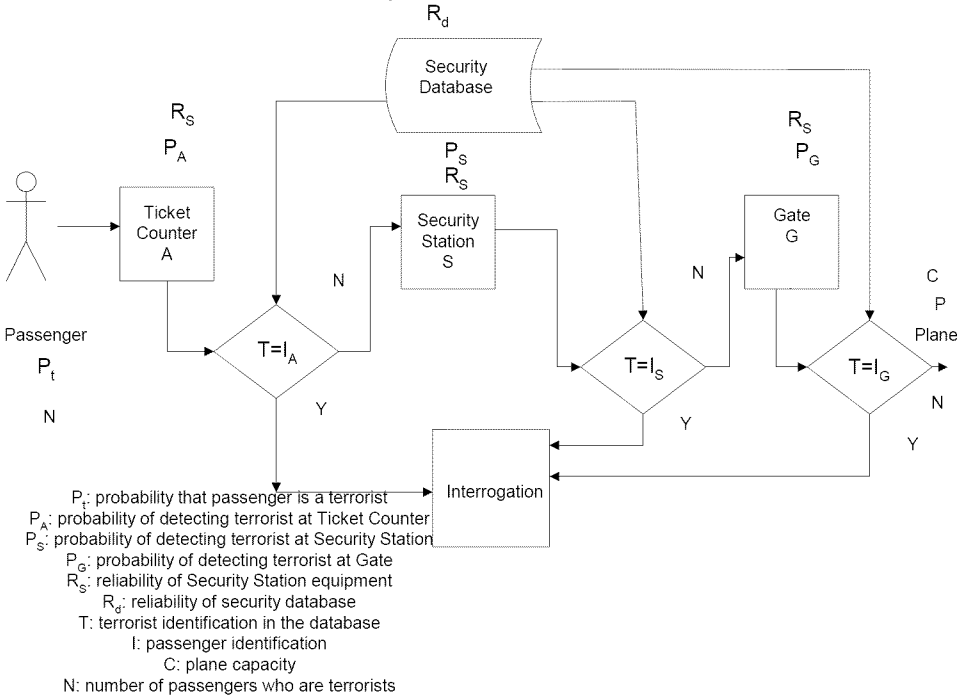
P_{Gf}, probability of *non detection* at the gate.

P_{Gs}, probability of detection at the gate.

R_{do}, overall reliability that is decomposed into the reliabilities of the primary and secondary security databases, R_{d1} and R_{d2}, respectively.

R_{so} overall reliability that is decomposed into the reliabilities of the primary and secondary security equipment, R_{s1} and R_{s2}, respectively.

Figure 0. Terrorist Flow Process



Assumption: The events and variables in the analysis are assumed to be independent. Thus, their probabilities can be multiplied. This assumption seems reasonable because there is no dependence among the events of security checking at the three facilities and facility reliabilities.

Terrorist Scenario

Before we begin the scenario, let us consider the fact that multiple checks against a database are needed, even if this seems counter intuitive, for the following reason:

Assume that X is not a Muslim, but is part of a terrorist plot. X has a ticket under a false name – the name of Y and a false photo ID with the name of Y. X passes the check at the airline check in counter. Next, X gives his ticket to Y, a Muslim, who has a photo ID. Y goes to the security station and presents "his ticket" and photo ID. Although Y's name on his ticket and ID match, a search of the database shows that the ticketed person, X, is not a Muslim, and Y is detained for further investigation. Of course, if the database contains Y's photo, X would have been stopped at the ticket counter, but the reviewer did not make this point.

Picture the scenario shown in Figure 0, where a passenger, who may have biological, chemical, or nuclear weapons in his luggage, stops first at the ticket counter (A) to check in. In this model, airline and security personnel access a security database that contains information about people who are considered possible security threats; their identification is designated by T. Passengers have identification I_A at the ticket counter, I_S at the security station, and I_G at the gate.

The reason for the three identifications is that a passenger could use a different identification at each facility. If a database check results in $T = I_A$, or $T = I_S$, or $T = I_G$, the passenger is detained for interrogation. At the start of the interrogation, the passenger is assumed to *not* be a terrorist; however, subsequent questioning may suggest otherwise. If the passenger passes the ticket counter check, he proceeds to the security station (S), which is staffed by TSA and airport personnel. The same database check process takes place again. Why? The reason is that no database and computer system is 100% reliable. It is possible that the passenger is a terrorist and the ticket counter check failed to reveal this fact. Of course, the converse is possible. This is why there should be presumed innocence at the start of the interrogation. Unfortunately, currently, the drivers license is the main means of passenger identification, and it is not standardized among the states. As Richard Clark points out, airline agents make no attempt to validate passenger identification [CLA05]. Perhaps, a national identification card is needed, but this might be considered a violation of civil liberties.

This process is repeated at the gate (G). If a terrorist manages to pass all three checks, he is allowed on board the aircraft. Of course, we want this event to have a very low probability. Subsequent sections will address how this could be achieved.

Events

The events pertinent to the process of terrorist detection are listed below.

1. Terrorist detected at ticket counter (A)
2. Terrorist *not* detected at ticket counter (A)
3. Terrorist detected at security station (S)
4. Terrorist *not* detected at security station (S)
5. Terrorist detected at gate (G)
6. Terrorist *not* detected at gate (G)

Definitions

The nomenclature of stations and their associated events are defined below.

A, S, and G are called stations

Events 1, 3, and 5 are independent (i.e., detection at a given station does not depend on detection at other stations).

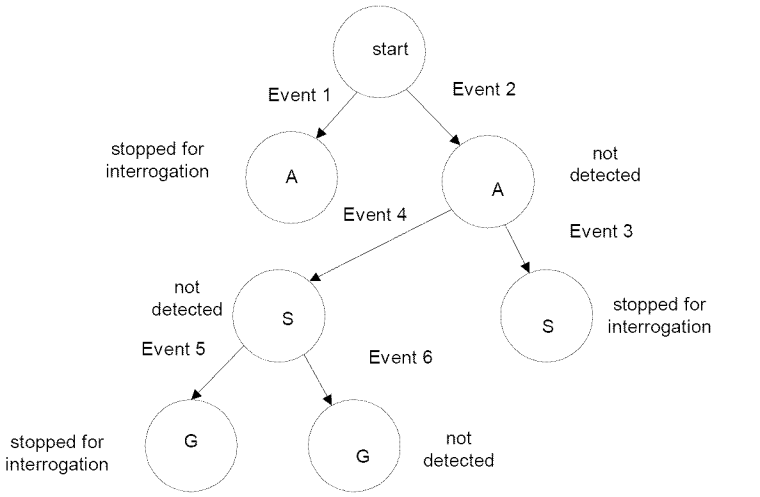
Events 2, 4, and 6 are independent (i.e., *non* detection at a given station does not depend on *non* detection at other stations).

Event Sequences

The sequence of events that transpire in the attempt to detect a terrorist is captures in the event transitions that follow.

A. Start → Event 1 → Terrorist stopped for interrogation at A
B. Start → Event 2 → Event 3 → Terrorist stopped for interrogation at S

Figure ASG. Airport Passenger Flow Diagram



Events

1 Terrorist detected at ticket counter (A)

2 Terrorist not detected at ticket counter (A)

3 Terrorist detected at security station (S)

4 Terrorist not detected at security station (S)

5 Terrorist detected at ticket gate (G)

6 Terrorist not detected at gate (G)

C. Start → Event 2 → Event 4 → Event 5 → Terrorist stopped for interrogation at G
D. Start → Event 2 → Event 4 → Event 6 → Terrorist *not* detected at A, S, and G

Event Sequences A, B, C, and D are independent (i.e., the fact that a terrorist is stopped at a given station does not depend on being stopped at other stations)

The event sequences A, B, C, and D and events 1, …, 6 in the passenger flow process are depicted in Figure *ASG*.

Probabilities

p: probability of terrorist *not* being detected on any given attempt at passing a *single* security check, independent of his location in the airport at any given time. This is a function of the accuracy and comprehensiveness of the security database and of the accuracy of security equipment (e.g., luggage x-ray equipment). Thus, p becomes the key probability in the model because we are modeling the process of the terrorist attempting to go undetected at the ticket counter, security station, and gate.

1 – p: probability of terrorist being detected on a given attempt at passing a *single* security check. This probability is also a function of the accuracy and comprehensiveness of the security database and of the accuracy of security equipment.

Binomial Distribution

The binomial distribution describes the possible number of times n that a particular event (e.g., terrorist *non* detection) will occur in a sequence of observations (e.g., at the ticket counter, security station, and gate). The binomial distribution is used when a researcher is interested in the probability of an event occurring. The binomial distribution is specified by the number of observations, x (e.g., number of times a passenger is subjected to a security check), and the probability of occurrence, which is denoted by p (e.g., probability of *non* detection).

Definitions

n trails: number of possible attempts by terrorist to avoid detection

n = 3 (A, S, G)

x: given number of attempts by terrorist to avoid detection

Apply Binomial Distribution

Our objective is to estimate the probability of non detection at A, S, and G, as a function of p, for the purpose of determining the threat posed by a terrorist at each of these stations. Therefore, we have, according to the binomial distribution,

$$P = \frac{n!}{x!(n-x)!} p^{x} (1-p)^{n-x} \qquad (1)$$

Why is it necessary to use the probability P when p has already been defined? The reason is that p does not take into account the *number of times* x that the terrorist attempts detection out of n = 3 possible attempts. The probability p only pertains to the event of *non* detection, *independent* of the number of attempts.

The following Table *Event* summarizes the application of the binomial distribution as it is applied to the quantities n, x, P, and p and the events 2, 4, 6, and 5, showing that the $\sum P$ exhausts the probability space.

Table Event. n = 3				
event		x	P	=
2	Not detected at A	1	$\frac{3!}{1!2!}p^1(1-p)^2$	$3\,p - 6\,p^2 + 3\,p^3$
4	Not detected at S	2	$\frac{3!}{2!1!}p^2(1-p)$	$3\,p^2 - 3\,p^3$
6	Not detected at G	3	$\frac{3!}{3!0!}p^3(1-p)^0$	P^3
5	detected at G	0	$\frac{3!}{0!3!}p^0(1-p)^3$	$1-3p+3p^2-p^3$
			Total	1

Probabilities of Events

In the sections that follow, we describe the airport security events, model the related probabilities of events, determine key points and values on the probability functions, and determine local minima and maxima of the functions by using the calculus. The key points and values, and the local minima and maxima, characterize the probability of non detection (our airport security metric), and identify the optimal non detection probabilities at the ticket counter, security station, and gate that imply policy decisions for government, airport, and airline managers. In developing an optimal solution, we strive for optimality across all entities and personnel within the scope of this research -- airlines; airport security personnel, security database, and equipment; FAA; and TSA – rather than a single entity [HIL01]. This is achieved by modeling the ticket counter, security station, and gate as a single integrated security system.

It is important to note that an "optimal solution" provided by a model may not br optimal in the eyes of the decision makers responsible for airport security. They are the final arbiters of what constitutes a good security policy {HIL01].

Event 2: Terrorist *not* detected at ticket counter (A)

x = 1 attempt at *non* detection at A; n =3 possible attempts

Applying the binomial distribution, the probability of Event 2 = P_{Af}:

$$P_{Af} = \frac{3!}{1!2!}p^1(1-p)^2 = 3p(1-p)^2 \qquad (2)$$

$$\mathbf{P_{Af} = 3\,p - 6\,p^2 + 3\,p^3} \qquad (3)$$

For $P_{Af} = 1$, $3p - 6p^2 + 3p^3 = 1$, $3p - 6p^2 + 3p^3 - 1 = 0$

(4)

Solving for the roots of (4), p = 1.475; this value is obviously infeasible

For $P_{Af} = 0$, p = 0, p = 1; only p = 0 is a realistic solution (i.e., P_{Af} should = 0 when p = 0; it should not equal 0 when p = 1). The rate of change of P_{Af} with p is given by equation (5):

$$\frac{dP_{Af}}{dp} = 3 - 12p + 9p^2 = 0 \;,\; 3p^2 - 4p + 1 = 0$$

(5)

$$p = \frac{4 \pm \sqrt{16 - 4(3)(1)}}{6} = \frac{4 \pm 2}{6} = \frac{2}{3} \pm \frac{1}{3}$$

(6)

$p_1 = 1$, $p_2 = 1 / 3$

$$\frac{d^2P_{Af}}{d^2p} = -12 + 18p$$

(7)

For $p_1 = 1$, $\frac{d^2P_{Af}}{d^2p} = -12 + 18 = 6 \Rightarrow P_{Af}$ minimum

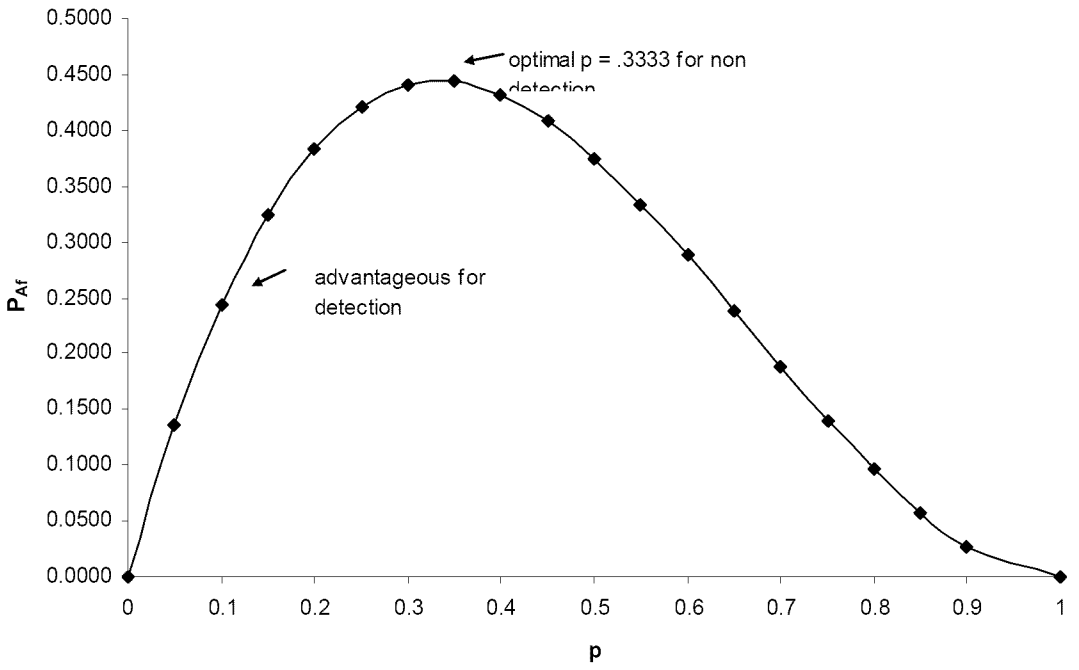
For $p_2 = .3333$, $\frac{d^2P_{Af}}{d^2p} = -12 + (18)(.3333) = -6.0 \Rightarrow P_{Af}$ **maximum**

For $p_1 = 1$, $P_{Af} = (3)(1) - (6)(1) + (3)(11) = 0$

For $p_2 = .35$, $P_{Af} = (3)(.3333) - (6)(.3333)^2 + (3)(.3333)^3 =$ **.4444**

As shown in Figure 1, where P_{Af} is plotted against p, the maximum value of P_{Af} = **.4444** occurs at p = **.3333**. After that, P_{Af} decreases with p, becoming 0 at p =1. The reason for the decrease is that the binomial representation of equation (2) is not only a function of probability of *non* detection p but also a function of the probability of detection (1-p) at the ticket counter. At p = .3333, p^1 begins to exceed $(1-p)^2$ in equation (2). Thus the optimal p represents the resolution of these counteracting factors. The policy implication suggested by this result is that the FAA, airport managers, and airline managers would attempt to improve security at ticket counters (e.g., use of computerized security database) so that p would be reduced to a value much lower than .3333.

Figure 1. Probability of Non Detection at Ticket Counter (P_{Af}) vs. p



Event 4: Terrorist *not* detected at security station (S)

x = 2 attempts at *non* detection at S; n =3 possible attempts

Applying the binomial distribution, the probability of Event 4 = P_{Sf}:

$$P_{Sf} = \frac{3!}{2!1!} p^2(1\text{-}p) = 3p^2(1\text{-}p) \qquad (8)$$

$$\mathbf{P_{Sf} = 3\ p^2 - 3\ p^3} \qquad (9)$$

For P_{Sf} =1, 3 p^2 – 3 p^3 = 1, 3 p^2 – 3 p^3 – 1 =0

Solving for the roots of (8), p = 1.264; this value is obviously infeasible

For P_{Sf} = 0, p = 0, p = 1; only p = 1 is realistic solution (i.e., P_{Sf} should = 0 when p = 0; it should not equal 0 when p = 1). The rate of change of P_{Sf} with p is given by equation (10):

$$\frac{dP_{Sf}}{dp} = 6p - 9p^2 = 0, 2p - 3p^2 = 0 \tag{10}$$

$$p = \frac{-2 \pm \sqrt{4 - 4(-30(0)}}{-6} = \frac{-2 \pm \sqrt{2}}{-6} = \frac{1}{3} \pm \frac{1.4192}{6}$$

$p_1 = .65$, $p_2 \approx 0$

$$\frac{d^2P_{Sf}}{d^2p} = 6 - 18p \tag{11}$$

For $p_1 =$ **.65**, $\frac{d^2P_{Sf}}{d^2p} = 6 - (18)(.65) = -5.7 \Rightarrow P_{Sf}$ **maximum**

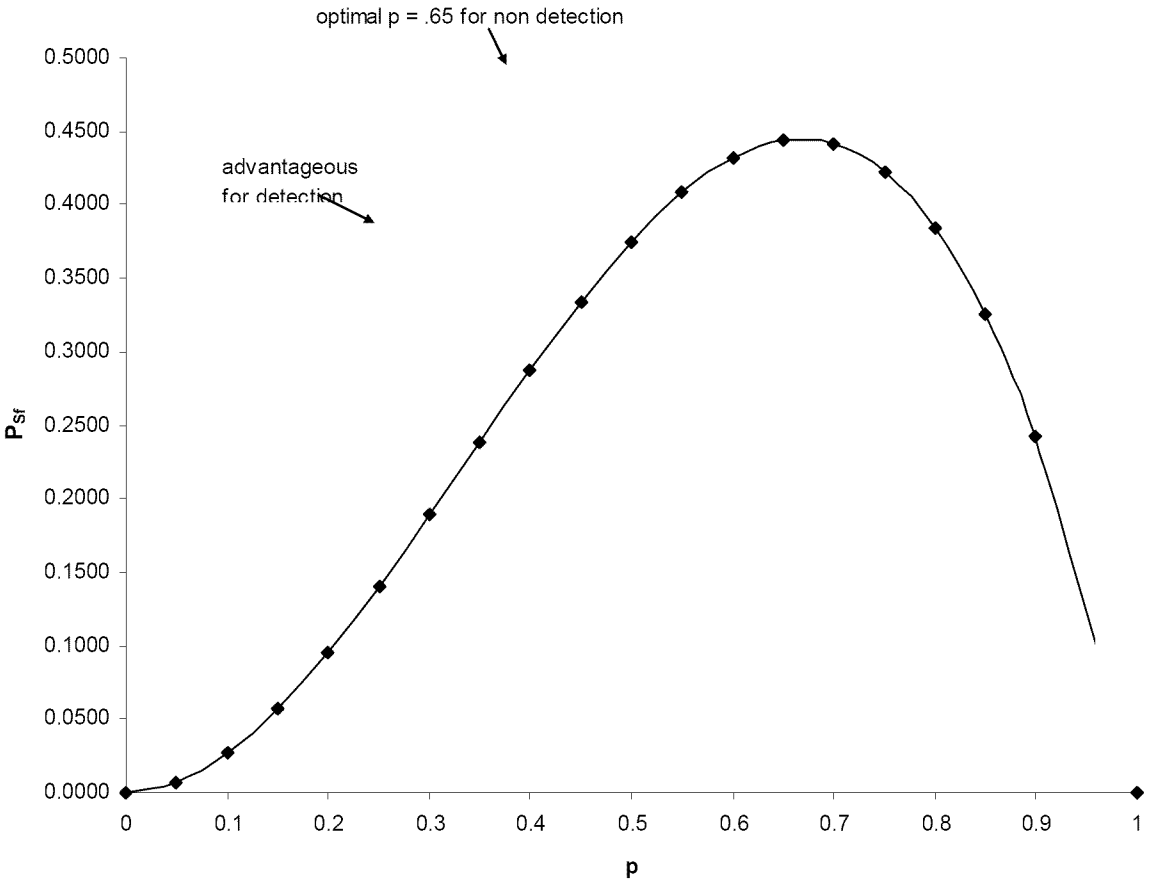
For $p_1 = 0$, $\frac{d^2P_{Sf}}{d^2p} = 6 - (18)(0) = 6 \Rightarrow P_{Sf}$ minimum

For $p_1 =$ **.65**, $P_{Sf} = (3)(.65)^2 - 3(.65)^3 =$ **.4436**

For $p_1 = 0$, $P_{Sf} = 0$

As shown in Figure 2, where P_{Sf} is plotted against p, the maximum value of $P_{Sf} =$ **.4436** occurs at p = **.65**. After that, P_{Sf} decreases with p, becoming 0 at p =1. The reason for the decrease is that, while the binomial representation of equation (2) increases with p, (1-p) -- the probability of terrorist being detected -- decreases with p. Thus the optimal p represents the resolution of these counteracting factors. The policy implication suggested by this result is that the FAA, airport managers, and TSA managers would attempt to improve security at security stations (e.g., use of computerized luggage checking system) so that p would be reduced to a value much lower than .65.

Figure 2. Probability of Non Detection at Security Station, P_{Sf}, vs. p



Event 6: Terrorist *not* Detected at gate (G)

x = 3 attempts at non detection out of n = 3 total attempts

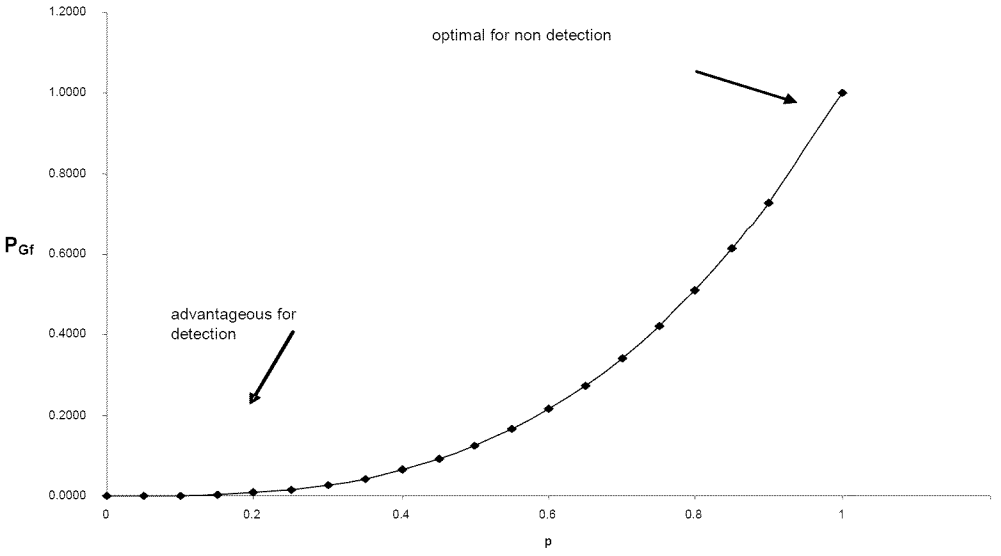
Applying the binomial distribution, the probability of Event 6 = P_{Gf}:

$$P_{Gf} = \frac{3!}{3!0!}p^3(1\text{-}p)^0 = p^3 \qquad (12)$$

As shown in Figure 3, where P_{Gf} is plotted against p, the maximum value of $P_{Gf} = 1.0$ occurs at p = 1.0. In this case, P_{Gf} increases monotonically. The reason for this is that there is only a p *non detection* term in equation (12); no 1-p detection term. The policy implication suggested by this result is that the FAA, airport managers, airline managers, and TSA managers would attempt to improve security at the ticket counters and at security stations to the extent that terrorists would be detected *before* they reach the gate, because after they reach the gate, there is little opportunity for detection, as shown in Figure 3.

Since the gate is the last place to stop the terrorist within the scope of the model -- P_{Gf} is our metric of the quality of the security system -- the lower the better – consistent with cost, personnel and technology constraints. Decision makers could gauge the performance of their security system against this metric [HIL01].

Figure 3. Probability of Non Detection at Gate, P_{Gf} vs. p



Event 5: Terrorist Detected at gate (G):

x = 0 attempts at *non detection* out of n = 3 total attempts is equivalent to a successful detection.

Applying the binomial distribution, the probability of Event 5 (successful detection at G) =

$$P_{Gs} = \frac{3!}{0!3!}p^0(1-p)^3 = 1-3p+3p^2-p^3 \qquad (13)$$

This is also equal to:

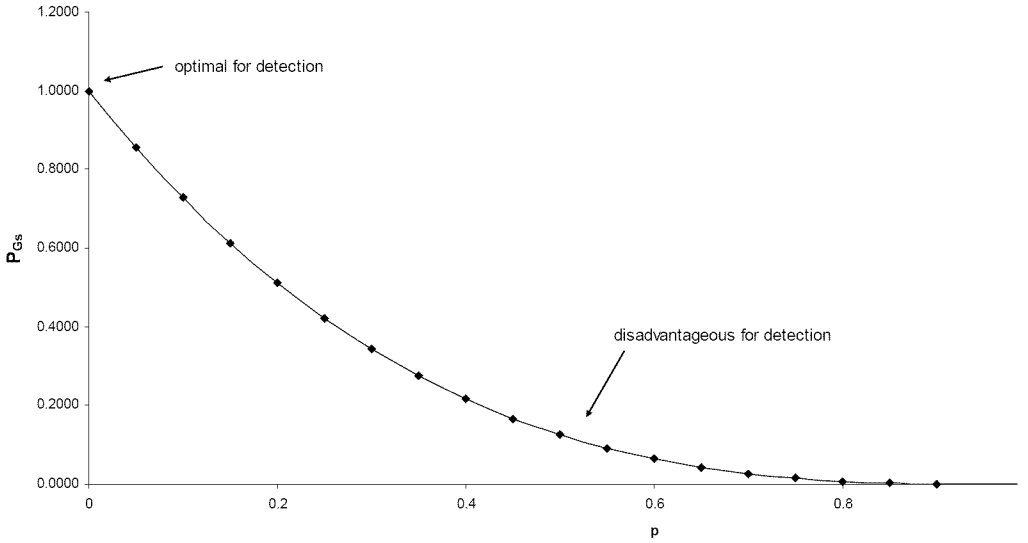
$$\mathbf{P_{Gs} = 1 - P_{Af} - P_{Sf} - P_{Gf} = 1 - (3\,p - 6\,p^2 + 3\,p^3) - (3\,p^2 - 3\,p^3) - p^3 = 1 - 3\,p + 3\,p^2 - p^3}$$

For $P_{Gs} = 1$, $1 - 3\,p + 3\,p^2 - p^3 = 1$, $-3\,p + 3\,p^2 - p^3 = 0$

Solving for the roots of (13), no feasible roots were found
For $P_{Gs} = 0$, $p = 0$

$$\frac{dP_{Gs}}{dp} = -3+6P-3p^2 = 0, 3p^2-6p+3=0, p^2-2p+1=0 \qquad (14)$$

Figure 4. Probability of Detection at Gate, P_{Gs}, vs. p



$$p=\frac{2\pm\sqrt{4-(4)(1)(1)}}{2}=\frac{2}{2}=1$$

$$\frac{d^2P_{Gs}}{d^2p}=6-6p, \text{for} p_1=1, \frac{d^2P_{Gs}}{d^2p}=0 \qquad (15)$$

$$\frac{d^3P_{Gs}}{d^3p}=-6\neq 0\text{, for } p_1=1,\ P_{Gs} \text{ is neither a minimum nor maximum} \qquad (16)$$

For $p_1=1$, $P_{Gs}=1-3+3-1=0$

For $p_2=0$, $P_{Gs}=1-0+0-0=1$

As shown in Figure 4, where P_{Gs} is plotted against p, the maximum value of P_{Gs} = 1.0 occurs at p = 0. In this case, P_{Gs} decreases monotonically. The reason for this is that there is only a 1 - p detection term in equation (13); no p *non detection* term. The policy implication suggested by this result is that the FAA, airport managers, and airline managers would attempt to improve security at the gate so that p is not significantly greater than 0, because P_{Gs} decreases rapidly thereafter, as shown in Figure 4.

Effectiveness of Detection at Gate

Now, we combine probability of *non detection* P_{Gs} with the reliability of the security database R_d and the reliability of the security equipment R_s to produce the effectiveness at the gate. Before we present this effectiveness equation, we elaborate on the characteristics of R_d and R_s, and show how redundancy increases reliability and, therefore, effectiveness.

Definitions

Definitions that characterize the redundant security database and security equipment, and their reliabilities are presented below.

d_1: primary security database
d_2: secondary security database
s_1: primary security equipment
s_2: secondary security equipment

R_{do}: overall reliability of security database
R_{d1}: reliability of primary security database
R_{d2}: reliability of secondary security database

R_{so}: overall reliability of security equipment
R_{s1}: reliability of primary security equipment (.96, 1.00, with a mean = .98 [CRS04]
R_{s2}: reliability of secondary security equipment (.96, 1.00, with a mean = .98 CRS04]

Assumptions

The assumptions upon which the computations of reliability rest are as follows:

d_1 and d_2 are independent (i.e., failure of d_2 does not affect reliability of d_1)

s_1 and s_2 are independent (i.e., failure of s_1 does not affect reliability of s_2)

Reliability Equations

The reliability of parallel components is computed below.

$R_{do} = R_{d1} + R_{d2} - R_{d1} R_{d2}$: reliability of two components in parallel (i.e., redundancy) (16)

$R_{so} = R_{s1} + R_{s2} – R_{s1} R_{s2}$: reliability of two components in parallel (i.e., redundancy) (17)

The redundancy characteristics are re-elaborated in Figures 5 and 6.

Data Values

Mean values of security database and security equipment reliabilities were obtained from Congressional Research Service reports as follows:

R_{d1}, R_{d2}, R_{s1}, R_{s2}: specified between 0 and 1, and randomized, with a mean ≅ .96 [CRS04]

Probability that the passenger is a terrorist = P_t: specified between 0 and 1, and randomized, with a mean ≅ .05 [CRS04]

Sensitivity Analysis

Randomization of R_{d1}, R_{d2}, R_{s1}, R_{s2}, and P_t, within the specified constraints, provides a degree of sensitivity analysis.

Effectiveness

The effectiveness of terrorist detection at the gate is obtained by melding P_{Gs} with the reliabilities obtained by redundant component analysis, as shown in equation (18).

Effectiveness is a better metric of ability to detect terrorists than P_{Gs} alone, because, whereas P_{Gs} is a function of the accuracy and speed of the database and equipment, it does not include reliability. If accuracy and speed are high, but reliability is low, overall effectiveness of detection will be low.

Effectiveness of security measures at the gate = E_G:

$$E_G = P_{Gs}\, R_{do}\, R_{So} = (1 - p)^3\, (R_{d1} + R_{d2} - R_{d1}\, R_{d2})\, (R_{s1} + R_{s2} - R_{s1}\, R_{s2}) \qquad (18)$$

Also, using equations (16) and (17), $E_G = (1- p)^3\ R_{do}\, R_{So}$

(19)

$$\frac{dE_G}{dp} = -3(1-p)^2 R_{do} R_{so} = 0, (1-p)^2 = 0, 1-2p+p^2 = 0, p_1 = 1, p_2 = 1$$

(21)

$$\frac{dE_G^2}{dp^2} = 6(1-p) R_{do} R_{so}$$

(22)

For $p_1 = p_2 = 1$, $\frac{dE_G^2}{dp^2} = 0$, $\Rightarrow$ neither minimum or maximum

For $p_1 = 1$, $E_{Gs} = 0$

For $p_2 = 0$, $E_G = R_{do}\, R_{So}$

The policy implication of Figure 7, where E_G is plotted against p is to make R_{d1}, R_{d2}, R_{s1}, R_{s2} as high as possible, because from equations (16) and (17), this will maximize R_{do} and R_{so}, respectively. Of course, this plan must be consistent with cost and technical considerations (i.e., state of the practice with respect to achieving reliability). Doing this will maximize E_G at probability of *non detection* = p = 0, as can be seen in Figure 7.

Figure 5. Redundancy in Security Database System
Primary Security Database Equipment

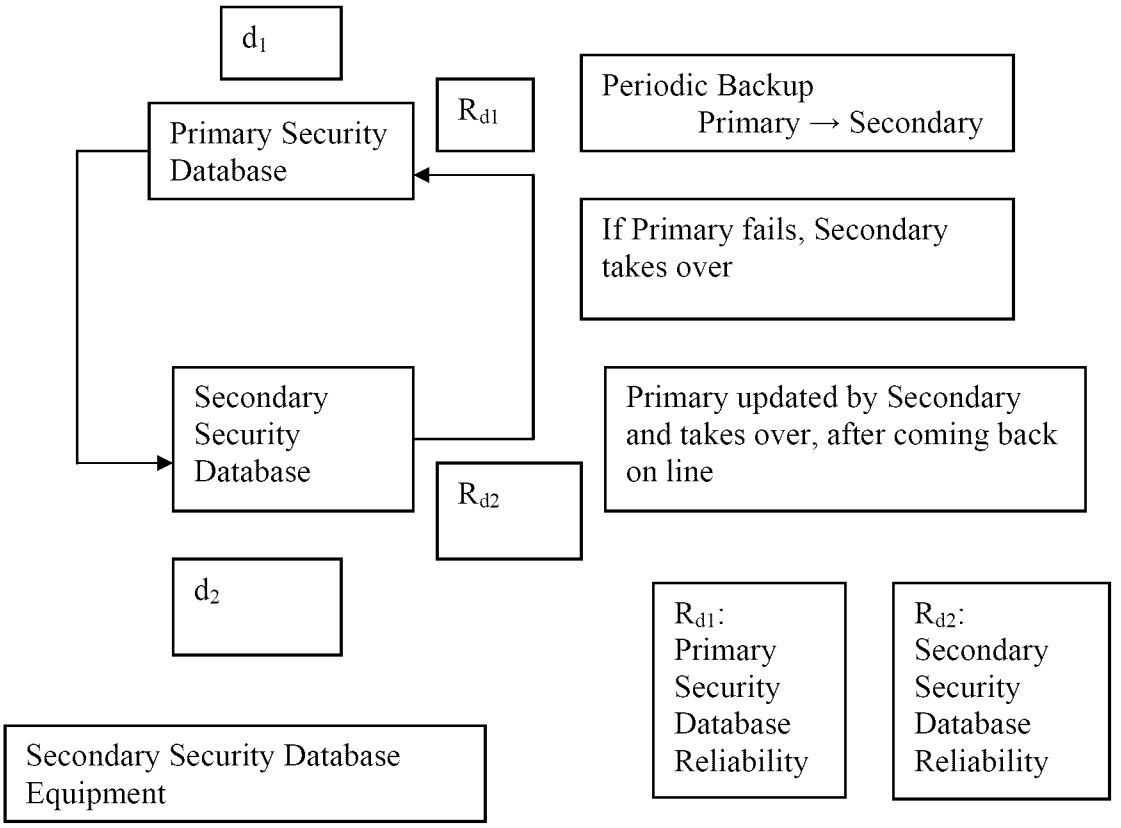
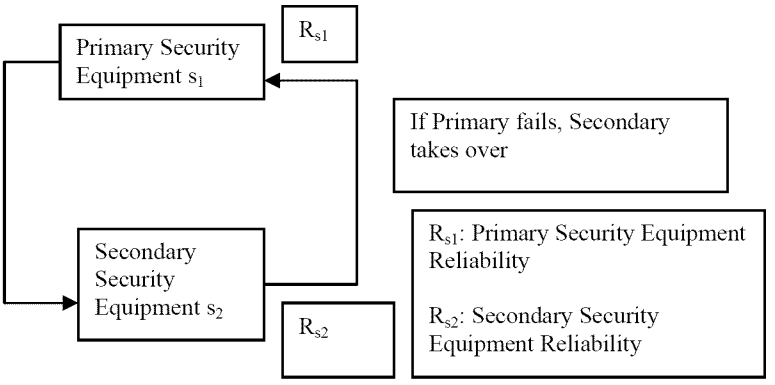


Figure 6. Redundancy in Security Equipment System



Evaluation of Relative Terrorist Threats at the Ticket Counter, Security Station, and Gate

Figure 8 quantifies what seems intuitive about a terrorist escaping detection at the ticket counter, security station, and gate. That, is the more stations that fail to detect the terrorist, the easier it is for him to go undetected at succeeding stations. In Figure 8, this is portrayed by the optimal probability of *non detection* p increasing from ticket counter to security station, and, finally, the probability of *non* detection increasing monotonically with p, at the gate. The policy implication is clear: stop the terrorist as soon as possible, preferably at the ticket counter. This objective is crucial when we consider that the terrorist's chances of achieving at least partial success (i.e., high probability of non detection) exceeds 75 per cent, according to [JOH91]. According to the model, as Figure 8 shows, this level of success would not be achieved at the ticket counter or security station but could be accomplished at the gate.

Unfortunately, the ticket counters are under the control of the airlines and are the entity least subject to control by the government. A compromise solution might be to emphasize detection at the security station because it is under the control of the TSA and airport management and has the advantage of containing luggage checking equipment and, in the future may be equipped with a security database, as an additional check on passengers.

Figure 7. Effectiveness of Detection at the Gate, E_G, vs. p

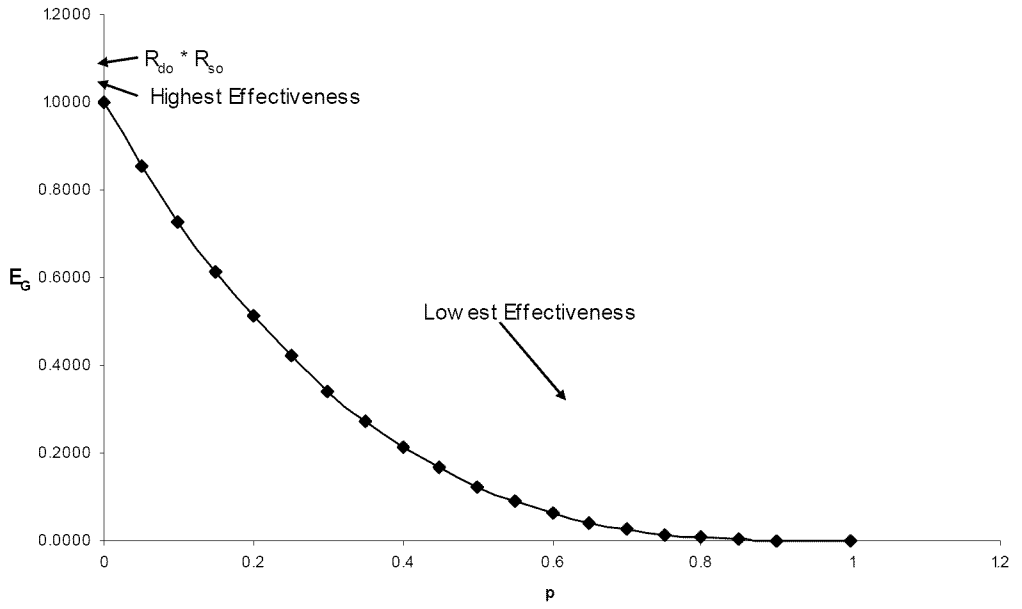
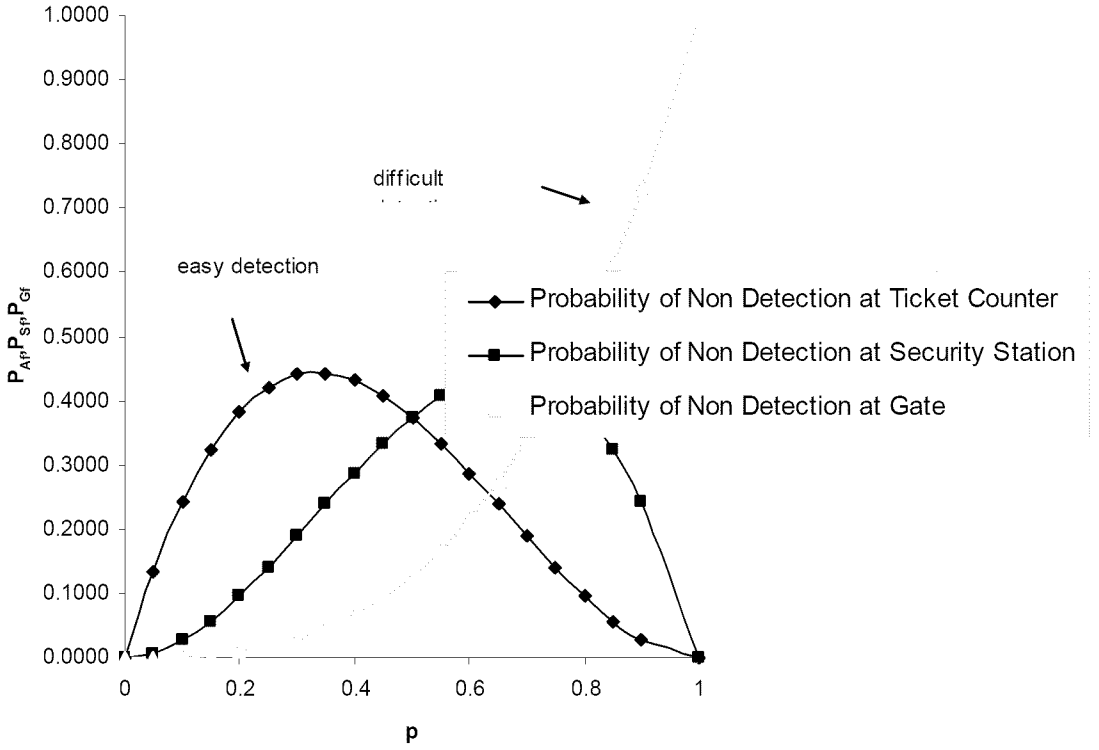


Figure 8. Probabilities of Non Detection vs. p



Actors and Facilities

As shown in Figure 0, the security process actors are airline ticket agents, security station personnel (TSA and airport luggage screeners), and airline personnel at the gate; not shown is the flight crew. The security measures exercised by the crew are beyond the scope of this research. For the security system to work, there must be communication and coordination among these actors. The 9/11 report states that better coordination between the FAA and the airlines is needed [911, p. 10]. In addition, as stated in [JOH91]: "Good airport security involves outthinking the terrorist. It also involves cooperation among all agencies that can, together, block security loopholes that begins with ticket purchase and ends when the plane takes off". In response, TSA is developing a computer network to tie together administrative, passenger screening, and baggage screening areas [DHS05].

The TSA has obvious influence over airport and airline security personnel. In the model, this is accomplished, in part, by the security database. This capability seems to be lacking in airports at present. In addition to the database, an important contributor to terrorist detection is the number and quality of airport screeners. With respect to the former, TSA reports that the number of screeners has dropped from 60,000 to 45,000 due to insufficient funding [CSI04]. An additional concern is that the DHS Inspector General issued a report in September 2004 stating that Federal screening improvements were needed in training, equipment, and technology, policy and procedures, and management and supervision [SEC05]. Improvements in equipment and

technology could be achieved by using highly reliable and effective security database and security equipment for checking carry on luggage, checked luggage, and cargo.

In the model, the flight crew does not have access to the database because airline personnel at the gate would provide a security check prior to passenger boarding. The gate represents a further opportunity for passenger security database checking, before the passenger boards [JOH91]. However, having a fourth security check on board the aircraft might be a feature to consider.

Information Flow

Information flow, as opposed to physical flow, which is shown in Figure 0, is shown in Figure 9. This figure shows the important quantities associated with queuing at the various security checking facilities. An objective of this section is to expose security vulnerabilities that may not have been recognized heretofore.

Definitions

Refer to Figure 9 when reading the definitions:

λ_A: mean rate at which passengers approach the ticket counter in passengers per minute

λ_S: passenger input rate at Security Station : mean rate at which passengers approach the security station in passengers per minute

λ_G: passenger input rate at Gate : mean rate at which passengers approach the gate in passengers per minute

μ_A :passenger service rate at Ticket Counter : mean rate passengers can be served at the ticket counter in passengers per minute

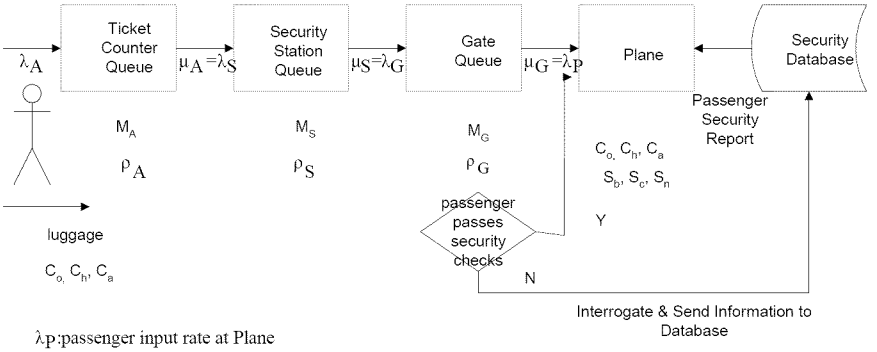
μ_S :passenger service rate at Security Station : mean rate passengers can go through the security check at the security station in passengers per minute

μ_G :passenger service rate at Gate : mean rate passengers can be boarded at the gate in passengers per minute

ρ_A :utilization at Ticket Counter : mean fraction of time that ticket counter is busy serving passengers

ρ_S :utilization at Security Station : mean fraction of time security station is busing doing security checks on passengers

Figure 9. Security Checking Information Flow



λ_P:passenger input rate at Plane

λ_A : passenger input rate at TicketCounter

λ_S: passenger input rate at Security Station

λ_G: passenger input rate at Gate

μ_A :passenger service rate at Ticket Counter

μ_S :passenger service rate at Security Station

μ_G :passenger service rate at Gate

M_A: number of servers at Ticket Counter

M_S: number of servers at Security Station

M_G: number of servers at Gate

ρ_A :utilization at Ticket Counter

ρ_S :utilization at Security Station

ρ_G :utilization at the Gate

C_o: carry on luggage

C_h: checked luggage

C_h: luggage for cargo bay

S_b: biological weapons

S_c: chemical weapons

S_n: nuclear weapons

ρ_G :utilization at the Gate : mean fraction of time that the agents at the gate are busy serving passengers

Passenger Security Processing Scenario

Passengers approach the ticket counter with a mean input rate of λ_A passengers per minute. The queue characteristics at the ticket counter are the number of agent stations (i.e., servers) M_A, queue utilization ρ_A, and queue service rate μ_A in passengers per minute. In addition, the terrorist could be carrying on luggage C_o, checking luggage C_h, or requesting that luggage be delivered to the cargo bay of the plane C_a. The concern about cargo has received increase emphasis of late because TSA is not only responsible for passenger security but cargo security as well [CSI04].

It is interesting to note the practice of El Al Airlines that first x-rays baggage destined for the cargo hold and then subjects it to depressurization to simulate flight conditions [JOH91]. The concept is that either the x-rays will expose weapons or depressurization will cause premature detonation. In addition, it has been recommended that vapor sniffing machines be added to the x-ray capability [JOH91].

Furthermore, "the success of TSA in fulfilling its aviation security mission depends heavily on the quality of its staff and the capability and reliability of the equipment (i.e., overall reliability R_s) to screen passengers and cargo in order to identify terrorists and terrorists' weapons, while minimizing disruption to public mobility and commerce "[SKI05].

Integrating Probability of Non Detection with Queue Characteristics

Now, we integrate the probability of *non* detection with the queue characteristics of the stations, such as the station service rate. Why would there be this relationship? The answer is that as the personnel at the stations are pressured to process passengers at increasing rates, their ability to detect terrorists decreases as they are distracted by the growing passenger flow rate. Therefore, we expect the probability of *non* detection to increase with increasing service rate (i.e., increasing number of passengers serviced per unit time).

To determine the mean input rate at the ticket counter λ_A, compute equation (23):

$$\lambda_A = C / t \tag{23}$$

where C = plane mean capacity = 400 passengers (assumed) and t is the time required to process passengers at the three facilities = 100 minutes (assumed). Therefore, λ_A = 4 passengers per minute (mean).

A security vulnerability could be created by the agents becoming overloaded by the size of the queue with the result that security checking becomes inadequate. Indeed, this very factor was discovered in the airports of Europe where passengers going through the screening process produced the assembly line effect, causing security personnel to become much less vigilant [JOH91]. This vulnerability is represented by the queue utilization ρ_A, as given by equation (24), taking into account the overall reliability of the security checking equipment R_{so}. Recall from Figure 0, that we are concerned with the reliability R_{so} of the ticket counter, security station, and gate. Thus, R_{so} appears in the queuing equations below.

From queuing theory [HIL01], we produce equation (24):

$$\rho_A = \frac{\lambda_A R_{so}}{\mu_A M_A} \tag{24}$$

Solving for μ_A yields equation (25):

$$\mu_A = \frac{\lambda_A R_{so}}{\rho_A M_A} \tag{25}$$

Since the service rate at the ticket counter μ_A = the input rate at the security station λ_S, (see Figure 9), we can develop equation (26) for the service rate μ_S at the security station:

$$\mu_S = \frac{\mu_A R_{so}}{\rho_S M_S} \qquad (26)$$

Since the service rate at the security station μ_S = the input rate at the gate λ_G, (see Figure 9), we can develop equation (27) for the service rate μ_G at the gate:

$$\mu_G = \frac{\mu_S R_{so}}{\rho_G M_G} \qquad (27)$$

Equations (25, 26, and 27) indicate that the vulnerability could be mitigated by reducing R_{so} or increasing the number of servers. Interestingly, reducing R_{so}, while helping to close this vulnerability, would decrease the *Effectiveness of Detection* at the gate! (see equation 18). Thus, there is a tradeoff between R_{so} and the number of servers, as they affect the *Effectiveness of Detection* and service rate, respectively.

At this point, we provide an *example*, to illustrate the analysis of the results of the example calculations of the relationships between service rate and number of servers, between probability of *non* detection and service rate, and between probability that the passenger is a terrorist and the estimated number of terrorists:

The data used in this *example* are the following:

$R_{so} = R_{s1} + R_{s2} - R_{s1} R_{s2}$: reliability of two components in parallel
(28)

R_{s1}, Rs2, Rs1, R_{s2}: mean ≈ .98

ρ_A = .8 (assumed from observation of ticket counter operations)

ρ_S = .9 (assumed from observation of security station operations: higher service rate requirement that ticket counter)

M_A = 1, …, 20

M_S = 1, …, 20

P_t = probability that passenger is a terrorist = N / C (on plane)
(29)

N= 0,…,10 terrorists on plane

C: Capacity of plane = number of passengers. See Table 1

Sample size = 10 or 20 depending on variable

Example Calculations

Ticket Counter

In Figure 10, we see that the service rate at the ticket counter μ_A decreases rapidly with the number of servers M_A, at first, but then decreases less rapidly later, reaching an optimal value at $\mu_A = .62$ passengers per minute; this occurs at $M_A = 8$ servers. The optimal μ_A is obtained from Figure 11, where the probability of *non* detection at ticket counter P_{Af} is maximum at $\mu_A = .62$. A possible explanation for this relationship in Figure 11 is that initially the ticket agents are unable to cope with the passenger input rate λ_A, thus allowing an increase in the probability of non detection P_{Af}. Eventually, at service rate $\mu_A = .62$, the agents adjust, get the security process under control, and P_{Af} decreases. The policy implication for airline managers is that providing more than eight agents, (see Figure 10), *from a security* standpoint, would be a waste of money and personnel. Of course, this may not be the correct policy from the standpoint of customer satisfaction.

Figure 10. Service Rate at Ticket Counter u_A vs. Number of Servers M_A

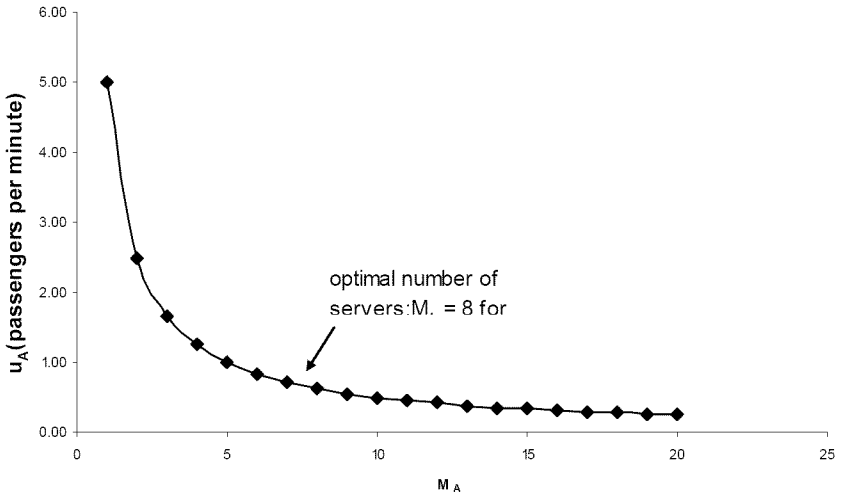
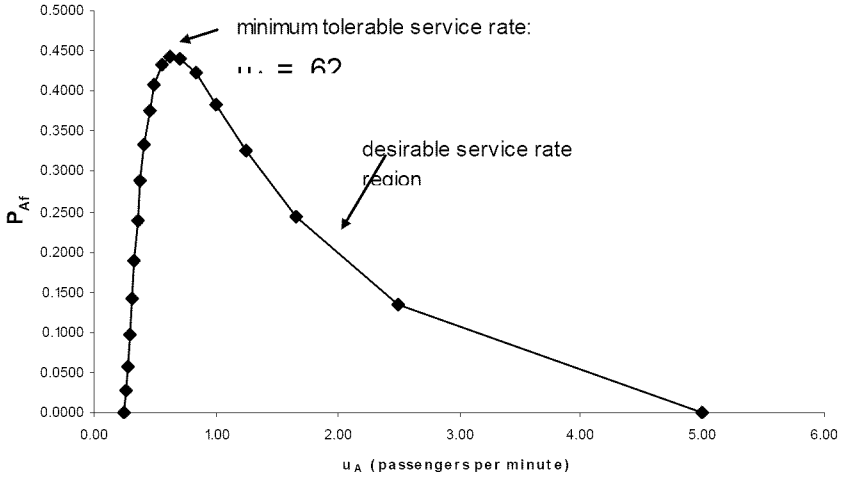


Figure 11. Probability of Non Detection at Ticket Counter, P_{Af}, vs. Service Rate u_A



Security Station

Figure 12, illustrates dramatically the danger in letting a terrorist past the ticket counter: In Figure 11, we saw that after the service rate at the ticket counter reached .62 passengers per minute, the probability of *non* detection steadily decreases. No such benign condition exists at the security station, where the probability of *non* detection increase monotonically with service rate. Therefore, the policy implication for airline and airport managers is to stop the terrorist at the ticket counter!

Analysis of Terrorist Factors

Figure 13 shows the relationship between the probability that a passenger is a terrorist P_t and the estimated number of passengers who are terrorists. We see that the P_t ranges between .001 and .039, for N ranging between 0 and 9, respectively; these are significant probabilities in light of the damage that terrorists did on 9/11, where a priori the probability of such a *successful* attack was considered insignificant. Therefore, since the number of terrorists, and their probabilities of occurrence, are areas not under the control of airport management, the policy implication is that they must be prepared to handle a number of incidents of high severity in the foreseeable future, and it behooves them to greatly improve the reliability and accuracy of detection hardware and software.

Figure 12. Probability of Non Detection at the Security Station, P_{Gf}, vs. Service Rate, u_S

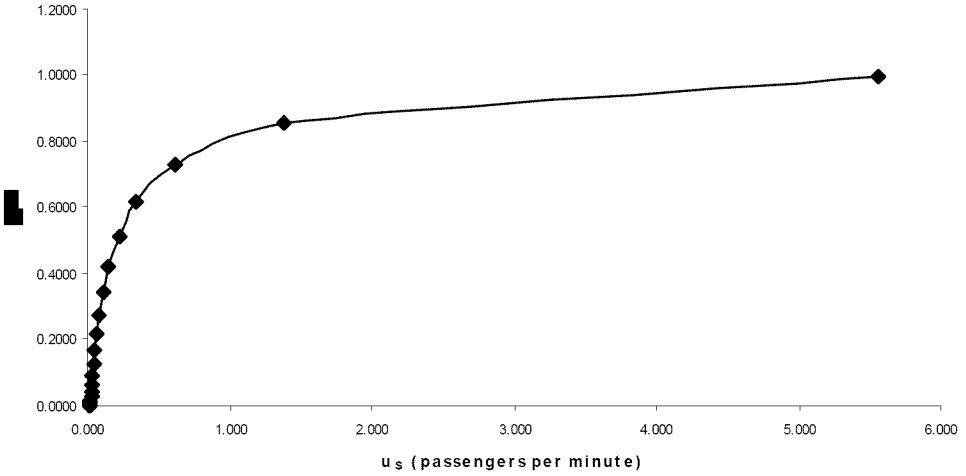
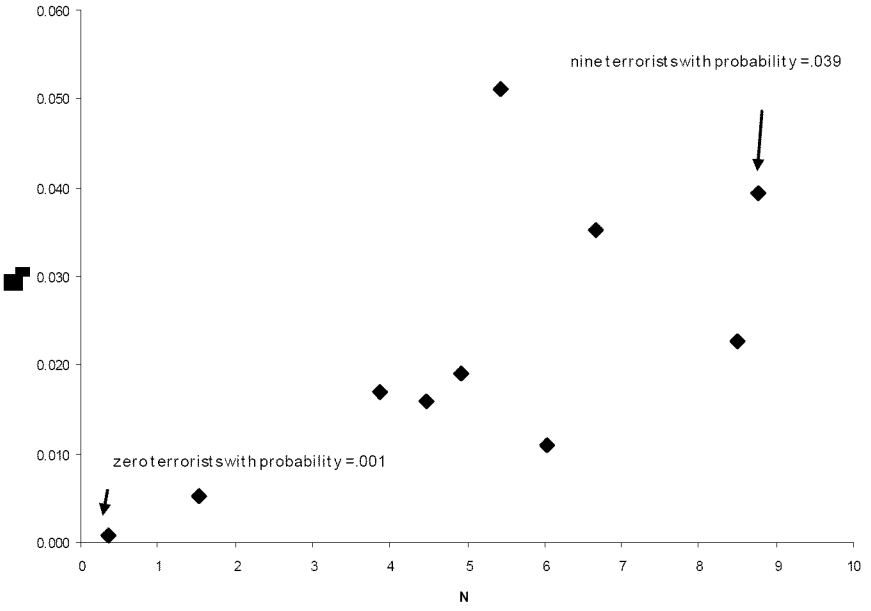


Figure 13. Probability that Passenger is a Terrorist, P_t, vs. Number of Terrorists, N



Countermeasures

Countermeasures to the threats, consistent with the previous section, involve the following:

Ticket Counter and Gate

Reduce the service rate of airline personnel at the ticket counter (μ_A) and gate (μ_G) by increasing the number of agents M_A, M_G, respectively. The first countermeasure may not be attractive to the airlines because of the personnel cost involved and limited space for additional personnel. The second countermeasure may be even less attractive because the number of gates is governed by airport design. More space could be considered when airports are redesigned or when new airports are constructed.

Security Station

Reduce the service rate of the security station (μ_S) by increasing the number of stations M_S. This option is attractive because the TSA controls TSA personnel and equipment and airport screeners. Thus, Congressional funding might be considered for more security personnel and equipment, airport space permitting.

Increase the reliability of the security station equipment Rs. This quantity influences security not only at the security station, but at the ticket counter and gate as well.

Security Database

As we have seen, the quality of the security database can have a pervasive effect on the ability to detect terrorists. Since the security database is accessed by all facilities, its reliability could be considered a high priority for Congressional funding.

What If Analysis

Terrorist with False Identification

One of the critical situations that would mitigate against terrorist detection: what if the terrorist carries a false identification? This means that the security database checks at the ticket counter, security station, and gate could fail. Then, the only facility to catch the terrorist is the x-ray equipment at the security station for checking luggage. The implication of this is that the terrorist could only be stopped at the security station. With only the luggage check to stop a terrorist, we now need a *probability of non detection* $P_{Sf} < .65$, as shown in Figure 8, for the security station, as opposed to a *probability of non detection* $P_{Af} < .35$, for the ticket counter, also shown in Figure 8. At the security station, P_{Sf} does not decline until .65, as opposed to P_{Af} declining at .35, in the case of the ticket counter. *If* the database check were working at the ticket counter, it would be easier to catch the terrorist there, as shown in Figure 8. However, what if the ticket counter security check is *not* working! What is the policy implication of this scenario? It means that the TSA and airport and airline managers need to operate as though the security

database will fail at all stations (even with redundant equipment), and the only line of defense is luggage x-ray equipment. Each manager must assess the security threat in a worst case scenario and guarantee that an adequate level of security is maintained.

Database and Equipment Failures

Another "what if" situation, with less adverse consequences than the above, is when the primary security database equipment d_1 fails or the primary security equipment s_1 fails. This adversity is covered by the redundant back up equipment d_2 and s_2, respectively. The implication for management in this case is to have a switchover and repair policy that can bring all units back on line as soon as feasible.

Security Station Performance

"What if" the queue characteristics that were evaluated in the "Integrating Probability of Non Detection with Queue Characteristics" section, do not hold. For example, what if we use the Department of Transportation goal that passenger wait time for security processing not exceed 10 minutes [CRS04] (e.g., at the security station): $t_{sw} \leq 10$ minutes.
Actually, the Bureau of Transportation Statistics found, in 2003 [CRS04], that $t_{sw} = 18$ minutes (mean). We will evaluate and compare the goal with the real world experience to note the effect of passenger wait time on the probability of *non* detection at the security station. Continuing the analysis, and noting that the reciprocal of the service time is equal to the service rate (i.e., $\mu_s = 1 / t_{ss}$), we have the following equations:

t_{st} = total time in security station system (wait time = t_{sw} + service time = t_{ss}) (30)

Case 1: $t_{sw} \leq 10$ minutes per passenger:

$$t_{st} \leq (10 + t_{ss}) \quad (31)$$

$$t_{ss} \geq (t_{st} - 10) \quad (32)$$

$$t_{st} \leq (1 / \mu_S) + 10 \text{ minutes per passenger} \quad (33)$$

Case 2: $t_{sw} = 18$ minutes per passenger (mean):

$$t_{st} = 18 + t_{ss} \quad (34)$$

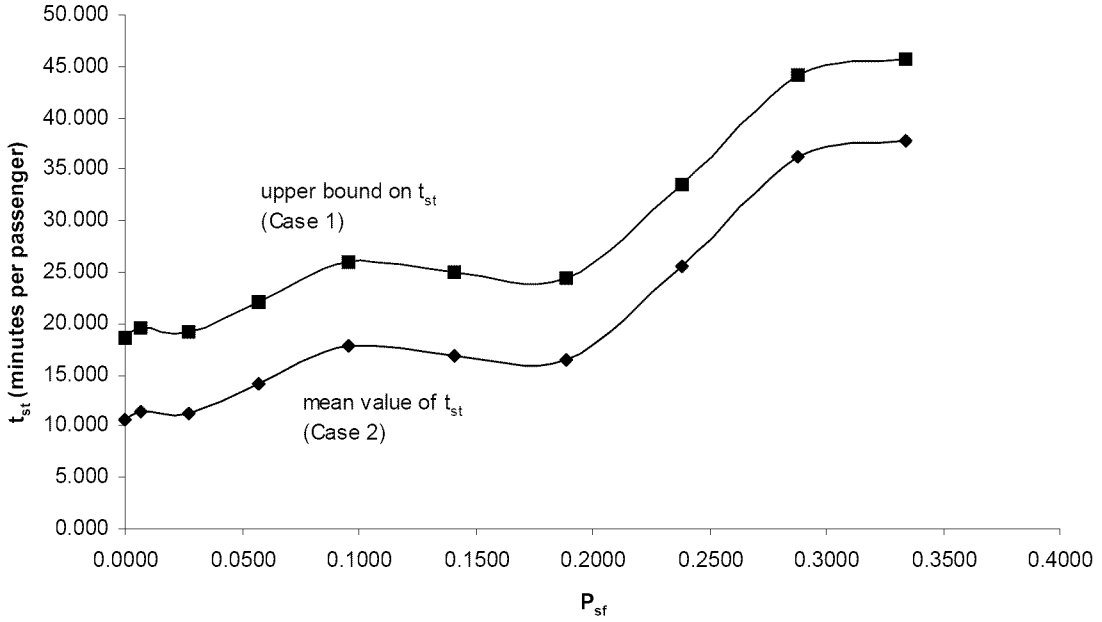
$$t_{ss} = t_{st} - 18 \quad (35)$$

$$t_{st} = (1 / \mu_S) + 18 \text{ minutes per passenger (mean)} \quad (36)$$

Now from equation (26), we have:

$$\mu_S = \frac{\mu_A R_{SO}}{\rho_S M_S}$$

Figure 14. Total Time of Security Check at Security Station, t_{st}, vs. Probability of Non Detection at Security Station, P_{Sf}



Combining (26) with (33), we obtain equations (37) for Case 1:

$$t_{st} \leq \frac{\rho_S M_S}{\mu_A R_{so}} + 10 \tag{37}$$

Combining (26) with (36), we obtain equations (38) for Case 2:

$$t_{st} = \frac{\rho_S M_S}{\mu_A R_{so}} + 18 \tag{38}$$

The results of this analysis are shown in Figure 14 for Case 1 (equation 37) and Case 2 (equation 38). The two curves are separated by a time of 8 minutes, as the two equations indicate. By providing upper bound and mean values, a band of total time of processing passengers t_{st} is provided that airport managers can use for estimating t_{st} for a given value of *probability of non detection* P_{Sf} at the security station. In addition, we note that if the managers lose control of passenger processing time, and it exceeds the allowable band, P_{Sf} will increase.

Conclusions

Based on the foregoing analysis that showed a preference for security improvements that could be implemented under Federal control and funding, we reach the following conclusions:

security station

Increase the accuracy and reliability of security checking equipment

Increase the number and quality of security personnel and servers

All Facilities

Implement, if the system does not exist, a high accuracy and reliable security database at the nation's airports

For existing databases, increase their accuracy and reliability

Maintain a centralized database of all passenger flight activity and perform security checks at all security points, using this database.

Include the use of fingerprints or photographs in the database of passengers as one way of positively identifying each passenger on each flight. However, this kind of surveillance would likely face serious legal and privacy challenges [BBC05].

.

Future Research Directions

The focus of future research will be to visit several major airports and hold discussions with airport managers for the purpose of collecting detailed security data and to obtain their opinions about the validity of the model. In addition, we will attempt to validate the model, based on the collected data, and to modify the model, if necessary.

References

[911] The 9/11 Commission Report: Final Report of the National Commission on Terrorist attacks upon the United States, Claitor's Publishing Division. Baton Rouge, LA, 2004.

[AIR] AirSafe.com (undated)

[BBC05] British Broadcasting Company, Thursday, 16 December, 2004, 12:21 GMT.

[BEN05] Rep. Bennie G. Thompson, Ranking Member, Committee on Homeland Security, U.S. House of Representatives, February 2005.

[CKE05] Clarke Kent Ervin, "A To-Do List for Chertoff", The Washington Post, Feb

[COR] Anthony H. Cordesman, Terrorism, Asymmetric Warfare, and Weapons of Mass Destruction: Defending the U.S. Homeland, Prager, Westport, CT, 2002.

[CLA05] Richard Clark, Former National Coordinator for Counter-terrorism, "Looking Back From 2011 – An Imagined History of the War on Terror", The Real State of the Union, Senate Russell Building 325, 1/7/05.

[CRS04] Congressional Reference Service Report for Congress, Aviation Security: Issues Before Congress Since September 11, 2001, Updated February 6, 2004, Bartholomew Elias.

[CSI04] David Heyman and James Jay Carafano, CSIS, DHS 2.0, Rethinking the Department of Homeland Security, The Heritage Foundation, December 13, 2004.

[DHS05] Budget in Brief, Department of Homeland Security, FY2006.

[HIL01] Fredrick S. Hillier and Gerald J. Lieberman, Introduction to Operations Research, Seventh Edition, M^{c}Graw Hill, 2001.

[HOU05] "Provisions of Immigration Bill", CQ Today, Friday. February 11, 2005.

[JOH91] Peter St. John, Air Piracy, Airport Security, & International Terrorism: Winning the War Against Hijackers, Quorum, 1991.

[MSN05] MSNBC.com, Report: FAA had many pre-9/11 warnings, The Associated Press, Updated: 1:05 p.m. ET Feb. 10, 2005.

[SEC05] "Security Swap", Government Executive, January 2005.

[SKI05] Statement of Richard L. Skinner, Acting Inspector General, U.S. Department Of Homeland Security, Before The Committee On Homeland Security And Governmental Affairs, United States Senate, January 26, 2005.

[USS05] U.S. Senate Committee on Homeland Security and Governmental Affairs, Pre-hearing Questionnaire for the Nomination of Michael Chertoff to be Secretary of Homeland Security.

[TUR93] Wayne C. Turner, et al, Introduction to Industrial and Systems Engineering, Third Edition, Prentice Hall, 1993.

[WAR05] Statement by Senator John Warner, R, VA, during the confirmation hearing for the nominee for Secretary of the Department of Homeland Security, February 2, 2005.

Appendix: Spreadsheet Data and Computations

p	P_{Af}	P_{Sf}	P_{Gf}	P_{Gs}	R_{d1}	R_{d2}	R_{s1}	R_{s2}	E_G
0	0.0000	0.0000	0.0000	1.0000	0.9942	0.9897	0.9822	0.9991	0.9999
0.05	0.1354	0.0071	0.0001	0.8574	0.9840	0.9776	0.9757	0.9608	0.8563
0.1	0.2430	0.0270	0.0010	0.7290	0.9708	0.9817	0.9892	0.9764	0.7284
0.15	0.3251	0.0574	0.0034	0.6141	0.9906	0.9910	0.9861	0.9983	0.6141
0.2	0.3840	0.0960	0.0080	0.5120	0.9901	0.9990	0.9819	0.9612	0.5116
0.25	0.4219	0.1406	0.0156	0.4219	0.9606	0.9757	0.9755	0.9937	0.4214
0.3	0.4410	0.1890	0.0270	0.3430	0.9858	0.9848	0.9617	0.9771	0.3426
0.35	0.4436	0.2389	0.0429	0.2746	0.9777	0.9940	0.9914	0.9950	0.2746
0.4	0.4320	0.2880	0.0640	0.2160	0.9655	0.9924	0.9704	0.9708	0.2158
0.45	0.4084	0.3341	0.0911	0.1664	0.9882	0.9756	0.9829	0.9705	0.1662
0.5	0.3750	0.3750	0.1250	0.1250	0.9660	0.9807	0.9826	0.9610	0.1248
0.55	0.3341	0.4084	0.1664	0.0911	0.9654	0.9994	0.9623	0.9831	0.0911
0.6	0.2880	0.4320	0.2160	0.0640	0.9805	0.9803	0.9832	0.9989	0.0640
0.65	0.2389	0.4436	0.2746	0.0429	0.9807	0.9844	0.9706	0.9987	0.0429
0.7	0.1890	0.4410	0.3430	0.0270	0.9683	0.9992	0.9750	0.9916	0.0270
0.75	0.1406	0.4219	0.4219	0.0156	0.9655	0.9673	0.9889	0.9875	0.0156
0.8	0.0960	0.3840	0.5120	0.0080	0.9882	0.9965	0.9905	0.9608	0.0080
0.85	0.0574	0.3251	0.6141	0.0034	0.9652	0.9669	0.9605	0.9652	0.0034
0.9	0.0270	0.2430	0.7290	0.0010	0.9974	0.9852	0.9940	0.9851	0.0010
1	0.0000	0.0000	1.0000	0.0000	0.9645	0.9697	0.9734	0.9752	0.0000
				mean	**0.9774**	**0.9846**	**0.9789**	**0.9805**	

R_{do}	R_{so}	M_A	μ_A	M_S	μ_S	M_G	μ_G	P_f	N	C
0.9999	1.0000	1	5.00	1	5.555	1	7.936	0.051	5	106
0.9996	0.9990	2	2.50	2	1.386	2	0.989	0.035	7	189
0.9995	0.9997	3	1.67	3	0.617	3	0.294	0.001	0	524
0.9999	1.0000	4	1.25	4	0.347	4	0.124	0.016	4	280
1.0000	0.9993	5	1.00	5	0.222	5	0.063	0.017	4	228
0.9990	0.9998	6	0.83	6	0.154	6	0.037	0.023	9	375
0.9998	0.9991	7	0.71	7	0.113	7	0.023	0.011	6	550
0.9999	1.0000	8	0.62	8	0.087	8	0.015	0.005	2	296
0.9997	0.9991	9	0.56	9	0.068	9	0.011	0.039	9	223
0.9997	0.9995	10	0.50	10	0.055	10	0.008	0.019	5	259
0.9993	0.9993	11	0.45	11	0.046	11	0.006			
1.0000	0.9994	12	0.42	12	0.039	12	0.005			
0.9996	1.0000	13	0.38	13	0.033	13	0.004			
0.9997	1.0000	14	0.36	14	0.028	14	0.003			
1.0000	0.9998	15	0.33	15	0.025	15	0.002			
0.9989	0.9999	16	0.31	16	0.022	16	0.002			
1.0000	0.9996	17	0.29	17	0.019	17	0.002			
0.9988	0.9986	18	0.28	18	0.017	18	0.001			
1.0000	0.9999	19	0.26	19	0.015	19	0.001			
0.9989	0.9993	20	0.25	20	0.014	20	0.001			
0.9996	**0.9996**									